CLAIMS

1. A denial-of-service attack defense system for protecting a communication device against a denial-of-service attack, the denial-of-service attack defense system comprising:

a monitoring device configured to be provided on a local area network to which the communication device that is a target of the denial-of-service attack is connected, the monitoring device monitoring a packet transmitted to the communication device via an internet-service-provider network; and

a restricting device configured to be provided on the internet-service-provider network, the restricting device restricting a packet to the local area network, wherein

the monitoring device includes

an attack detecting unit that detects an attack by the packet on the communication device; and

a protection-request-information transmitting unit that transmits protection request information indicating a request for protection against the attack to the restricting device, and

the restricting device includes a packet restricting unit that restricts a packet transmitted to the communication device via the internet-service-provider network based on the protection request information.

2. The denial-of-service attack defense system according to claim 1, wherein

the monitoring device further includes a signature generating unit that generates a signature indicating a feature of a packet that attacks the communication device,

the protection-request-information transmitting unit transmits the protection request information including the

signature to the restricting device, and

the packet restricting unit of the restricting device restricts a packet corresponding to the signature, which is to be transmitted to the communication device.

3. The denial-of-service attack defense system according to claim 2, wherein

the restricting device further includes a signature determining unit that determines whether the protection request information including the signature is appropriate, and

the packet restricting unit restricts a packet corresponding to a signature that is determined to be appropriate by the signature determining unit, which is to be transmitted to the communication device, and does not restrict a packet corresponding to a signature that is determined to be inappropriate, which is to be transmitted to the communication device.

4. The denial-of-service attack defense system according to claim 2 or 3, wherein

the restricting device further includes

a report generating unit that generates a report on a feature and an amount of a packet corresponding to the signature; and

a report transmitting unit that transmits the report to the monitoring device,

the signature generating unit generates a new signature based on the report,

the protection-request-information transmitting unit transmits the protection request information including the new signature to the restricting device, and

the packet restricting unit restricts a packet

corresponding to the new signature, which is to be transmitted to the communication device.

5. The denial-of-service attack defense system according to claim 4, wherein

the restricting device further includes a forwarding unit that forwards the protection request information to other restricting device provided on the internet-service-provider network, and

the forwarding unit determines whether to forward the protection request information based on the report generated at the report generating step, and forwards the protection request information to the other restricting device upon determining that it is necessary to forward the protection request information.

6. The denial-of-service attack defense system according to claim 3, wherein

the restricting device further includes a determination-result transmitting unit that transmits a result of determination of the signature determining unit to the monitoring device, and

when the result of determination indicates that the signature is inappropriate, the signature generating unit of the monitoring device generates, based on the result of determination, a new signature indicating the feature of the packet that attacks the communication device.

7. A denial-of-service attack defense method of protecting a communication device against a denial-of-service attack using a monitoring device and a restricting device, the monitoring device being configured to be provided on a local area network to which the communication

device that is a target of the denial-of-service attack is connected and monitoring a packet transmitted to the communication device via an internet-service-provider network, the restricting device being configured to be provided on the internet-service-provider network and restricting a packet to the local area network, the denial-of-service attack defense method comprising:

an attack detecting step of detecting including the monitoring device detecting an attack by the packet on the communication device;

a protection-request-information transmitting step of transmitting protection request information indicating a request for protection against the attack to the restricting device; and

a packet restricting step of restricting a packet transmitted to the communication device via the internet-service-provider network based on the protection request information.

8. The denial-of-service attack defense method according to claim 7, further comprising:

a signature generating step of generating including the monitoring device generating a signature indicating a feature of a packet that attacks the communication device, wherein

the protection-request-information transmitting step includes transmitting the protection request information including the signature to the restricting device, and

the packet restricting step includes restricting a packet corresponding to the signature, which is to be transmitted to the communication device.

9. The denial-of-service attack defense method according

to claim 8, further comprising:

a signature determining step of determining including the restricting device determining whether the protection request information including the signature is appropriate, wherein

the packet restricting includes

restricting a packet corresponding to a signature that is determined to be appropriate at the signature determining step, which is to be transmitted to the communication device; and

not restricting a packet corresponding to a signature that is determined to be inappropriate, which is to be transmitted to the communication device.

10. The denial-of-service attack defense method according to claim 8 or 9, further comprising:

the report generating step of generating including the restricting device generating a report on a feature and an amount of a packet corresponding to the signature; and

a report transmitting step of transmitting including the restricting device transmitting the report to the monitoring device, wherein

the signature generating step includes generating a new signature based on the report,

the protection-request-information transmitting step includes transmitting the protection request information including the new signature to the restricting device, and

the packet restricting step includes restricting a packet corresponding to the new signature, which is to be transmitted to the communication device.

11. A denial-of-service attack defense program for protecting a communication device against a denial-of-

service attack using a monitoring device and a restricting device, the monitoring device being configured to be provided on a local area network to which the communication device that is a target of the denial-of-service attack is connected and monitoring a packet transmitted to the communication device via an internet-service-provider network, the restricting device being configured to be provided on the internet-service-provider network and restricting a packet to the local area network, the denial-of-service attack defense program causing a computer to execute:

an attack detecting procedure of detecting including the monitoring device detecting an attack by the packet on the communication device;

a protection-request-information transmitting procedure of transmitting protection request information indicating a request for protection against the attack to the restricting device; and

a packet restricting procedure of restricting a packet transmitted to the communication device via the internet-service-provider network based on the protection request information.

12. The denial-of-service attack defense program according to claim 11, further causing the computer to execute:

a signature generating procedure of generating including the monitoring device generating a signature indicating a feature of a packet that attacks the communication device, wherein

the protection-request-information transmitting procedure includes transmitting the protection request information including the signature to the restricting device, and

the packet restricting procedure includes restricting a packet corresponding to the signature, which is to be transmitted to the communication device.

13. The denial-of-service attack defense program according to claim 12, further causing the computer to execute:

a signature determining procedure of determining including the restricting device determining whether the protection request information including the signature is appropriate, wherein

the packet restricting includes

restricting a packet corresponding to a signature that is determined to be appropriate at the signature determining step, which is to be transmitted to the communication device; and

not restricting a packet corresponding to a signature that is determined to be inappropriate, which is to be transmitted to the communication device.

14. The denial-of-service attack defense program according to claim 12 or 13, further causing the computer to execute:

a report generating procedure of generating including the restricting device generating a report on a feature and an amount of a packet corresponding to the signature; and

a report transmitting procedure of transmitting including the restricting device transmitting the report to the monitoring device, wherein

the signature generating procedure includes generating a new signature based on the report,

the protection-request-information transmitting procedure includes transmitting the protection request information including the new signature to the restricting device, and

the packet restricting procedure includes restricting a packet corresponding to the new signature, which is to be transmitted to the communication device.